CLAIMS:

What is claimed is:

1. A method of upgrading the integrity of a first timestamp having a first digital signature, the method comprising:

computing a hash value of the first digital signature;

combining the hash value with a current time value to form a second data item;

computing a second digital signature based on the second data item; and

combining the second data item and the second digital signature to form a second timestamp.

2. The method of claim 1, wherein computing the hash value, combining the hash value with the current time value, computing the second digital signature, and combining the second data item and the second digital signature are performed in response to a determination that the integrity of the first digital signature may soon become able to be compromised.

3. The method of claim 1, further comprising writing the second timestamp to a storage medium.

4. The method of claim 3, further comprising writing the first timestamp to the storage medium.

5. The method of claim 3, wherein the storage medium is memory.

6. The method of claim 3, wherein the storage medium is one of a disk and tape.

7. A method of upgrading the integrity of a first timestamp of a document, wherein the first timestamp includes a first hash value computed with a first hash function, the method comprising:

calculating a second hash value of the document using a second hash function;

combining the second hash value with a current time value to form a data item;

computing a digital signature of the data item; and

combining the digital signature and the data item to form a second timestamp.

8. The method of claim 7, wherein computing the second hash value, combining the second hash value with the current time value, computing the digital signature, and combining the data item with the digital signature are performed in response to a determination that the integrity of the first hash value may soon become able to be compromised.

9. The method of claim 7, further comprising writing the second timestamp to a storage medium.

10. The method of claim 9, further comprising writing the first timestamp to the storage medium.

11. The method of claim 9, wherein the storage medium is memory.

12. The method of claim 9, wherein the storage medium is one of a disk and tape.

13. A method of verifying the integrity of an upgrade timestamp associated with an earlier timestamp, comprising:

verifying integrity of a first digital signature associated with the upgrade timestamp;

calculating a first hash value of a second digital signature associated with the earlier timestamp; and

verifying that the first hash value matches a second hash value associated with the upgrade timestamp.

14. The method of claim 13, further comprising:

verifying integrity of the earlier timestamp.

15. The method of claim 14, wherein verifying the integrity of the earlier timestamp includes:

verifying integrity of the second digital signature;

calculating a third hash value of a document associated with the earlier timestamp; and

verifying that the third hash value matches a fourth hash value associated with the earlier timestamp.

16. A method comprising:

verifying integrity of each of a plurality of digital signatures, wherein each of the plurality of digital signatures signs a timestamp, and each timestamp includes a hash value of a common document, each hash value having been calculated with a different hash function.

17. A computer program product in a computer readable medium for upgrading the integrity of a first timestamp having a first digital signature, comprising functional descriptive data that, when executed by a computer, enables the computer to perform acts including:

computing a hash value of the first digital signature;

combining the hash value with a current time value to form a second data item;

computing a second digital signature based on the second data item; and

combining the second data item and the second digital signature to form a second timestamp.

18. The computer program product of claim 17, wherein computing the hash value, combining the hash value with the current time value, computing the second digital signature, and combining the second data item and the second digital signature are performed in response to a determination that the integrity of the first digital signature may soon become able to be compromised.

19. The computer program product of claim 17, comprising additional functional descriptive data that, when executed by the computer, enables the computer to perform additional acts including:

writing the second timestamp to a storage medium.

20. The computer program product of claim 19, comprising additional functional descriptive data that, when executed by the computer, enables the computer to perform additional acts including:

writing the first timestamp to the storage medium.

21. The computer program product of claim 19, wherein the storage medium is memory.

22. The computer program product of claim 19, wherein the storage medium is one of a disk and tape.

23. A computer program product in a computer readable medium, for upgrading the integrity of a first timestamp of a document, wherein the first timestamp includes a first hash value computed with a first hash function, comprising functional descriptive data that, when executed by a computer, enables the computer to perform acts including:

calculating a second hash value of the document using a second hash function;

combining the second hash value with a current time value to form a data item;

computing a digital signature of the data item; and

combining the digital signature and the data item to form a second timestamp.

24. The computer program product of claim 23, wherein computing the second hash value, combining the second hash value with the current time value, computing the digital signature, and combining the data item with the digital signature are performed in response to a determination that the integrity of the first hash value may soon become able to be compromised.

25. The computer program product of claim 23, comprising additional functional descriptive data that, when executed by the computer, enables the computer to perform additional acts including:
writing the second timestamp to a storage medium.

26. The computer program product of claim 25, comprising additional functional descriptive data that, when executed by the computer, enables the computer to perform additional acts including:
writing the first timestamp to the storage medium.

27. The computer program product of claim 25, wherein the storage medium is memory.

28. The computer program product of claim 25, wherein the storage medium is one of a disk and tape.

29. A computer program product in a computer-readable medium, for verifying the integrity of an upgrade timestamp associated with an earlier timestamp, comprising functional descriptive data that, when executed by a computer, enables the computer to perform acts including:

verifying integrity of a first digital signature associated with the upgrade timestamp;

calculating a first hash value of a second digital signature associated with the earlier timestamp; and

verifying that the first hash value matches a second hash value associated with the upgrade timestamp.

30. The computer program product of claim 29, comprising additional functional descriptive data that, when executed by the computer, enables the computer to perform additional acts including:

verifying integrity of the earlier timestamp.

31. The computer program product of claim 30, wherein verifying the integrity of the earlier timestamp includes:

verifying integrity of the second digital signature;

calculating a third hash value of a document associated with the earlier timestamp; and

verifying that the third hash value matches a fourth hash value associated with the earlier timestamp.

32. A computer program product in a computer-readable medium, comprising functional descriptive data that, when

executed by a computer, enables the computer to perform acts including:

verifying integrity of each of a plurality of digital signatures, wherein each of the plurality of digital signatures signs a timestamp, and each timestamp includes a hash value of a common document, each hash value having been calculated with a different hash function.

33. A data processing system for upgrading the integrity of a first timestamp having a first digital signature, comprising means for:

computing a hash value of the first digital signature;

combining the hash value with a current time value to form a second data item;

computing a second digital signature based on the second data item; and

combining the second data item and the second digital signature to form a second timestamp.

34. The data processing system of claim 33, wherein computing the hash value, combining the hash value with the current time value, computing the second digital signature, and combining the second data item and the second digital signature are performed in response to a determination that the integrity of the first digital signature may soon become able to be compromised.

35. The data processing system of claim 33, comprising additional means for writing the second timestamp to a storage medium.

36. The data processing system of claim 35, comprising additional means for writing the first timestamp to the storage medium.

37. The data processing system of claim 35, wherein the storage medium is memory.

38. The data processing system of claim 35, wherein the storage medium is one of a disk and tape.

39. A data processing system for upgrading the integrity of a first timestamp of a document, wherein the first timestamp includes a first hash value computed with a first hash function, the data processing system comprising means for:

calculating a second hash value of the document using a second hash function;

combining the second hash value with a current time value to form a data item;

computing a digital signature of the data item; and

combining the digital signature and the data item to form a second timestamp.

40. The data processing system of claim 39, wherein computing the second hash value, combining the second hash value with the current time value, computing the

digital signature, and combining the data item with the digital signature are performed in response to a determination that the integrity of the first hash value may soon become able to be compromised.

41. The data processing system of claim 39, comprising additional means for writing the second timestamp to a storage medium.

42. The data processing system of claim 41, comprising additional means for writing the first timestamp to the storage medium.

43. The data processing system of claim 41, wherein the storage medium is memory.

44. The data processing system of claim 41, wherein the storage medium is one of a disk and tape.

45. A data processing system for verifying the integrity of an upgrade timestamp associated with an earlier timestamp, comprising means for:

verifying integrity of a first digital signature associated with the upgrade timestamp;

calculating a first hash value of a second digital signature associated with the earlier timestamp; and

verifying that the first hash value matches a second hash value associated with the upgrade timestamp.

46. The data processing system of claim 45, comprising additional means for:

verifying integrity of the earlier timestamp.

47. The data processing system of claim 46, wherein verifying the integrity of the earlier timestamp includes:

verifying integrity of the second digital signature;

calculating a third hash value of a document associated with the earlier timestamp; and

verifying that the third hash value matches a fourth hash value associated with the earlier timestamp.

48. A data processing system comprising means for:

verifying integrity of each of a plurality of digital signatures, wherein each of the plurality of digital signatures signs a timestamp, and each timestamp includes a hash value of a common document, each hash value having been calculated with a different hash function.